WHAT IS CLAIMED IS:

1. A secure transaction process, comprising
generating a key from a user-supplied unencrypted password,
encrypting the user's password with the key,
creating a user record,
storing the encrypted password in the user record.

2. The process of claim 1, further comprising
upon user login, generating a key from a would-be user's password using the same algorithm used to generate the key from the originally supplied unencrypted password,
retrieving the corresponding user record,
decrypting the encrypted password in the user record using the key,
comparing the decrypted password with the would-be user-supplied password to see if they match.

3. The process of claim 2, further comprising
if the decrypted password and user-supplied password match, creating a temporary session record and storing the key in the session record, otherwise aborting the user login.

4. The process of claim 3, further comprising
encrypting other sensitive user data using the key and storing the encrypted data in the user record,
during a session wherein a session record has been created, using the key stored in the session record to decrypt other encrypted information stored in the user record for use in carrying out some desired action.

5. The process of claim 1, further comprising
generating a public/private key pair,

storing the public key on an application server and the mating private key only another server,

encrypting the original user-supplied unencrypted password with the public key and storing the public-key encrypted password on the application server,

fetching the private key from the other server and using it to decrypt selected information on the one server.

6. The process of claim 5, further wherein the other server is a secure off-site server.

7. A secure transaction process, comprising

generating an encryption key from user-supplied identification data,

encrypting the user's identification data with the key,

creating a user record,

storing the encrypted identification data in the user record.

8. The process of claim 7, further comprising

upon user login, generating a key from a would-be user's identification data supplied at login using the same algorithm used to generate the key from the originally supplied unencrypted identification data,

retrieving the corresponding user record,

decrypting the encrypted identification data in the user record using the key,

comparing the decrypted identification data with the would-be user-supplied identification data to see if they match.

9. The process of claim 8, further comprising

if the decrypted identification data and user-supplied identification data match, creating a temporary session record and storing the key in the session record, otherwise aborting the user login.

10. The process of claim 9, further comprising

encrypting other sensitive user data using the key and storing the encrypted data in the user record,

during a session wherein a session record has been created, using the key stored in the session record to decrypt other encrypted information stored in the user record for use in carrying out some desired action.